Checklist
Personal data breaches

Preparing for a personal data breach

 We know how to recognise a personal data breach.

 We understand that a personal data breach isn't only about loss or theft of personal data.

 We have prepared a response plan for addressing any personal data breaches that occur.

 We have allocated responsibility for managing breaches to a dedicated person or team.

 Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

 We have in place a process to assess the likely risk to individuals as a result of a breach.

 We know who is the relevant supervisory authority for our processing activities (see Data Audit).

 We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet. (see pg. 4)

 We know what information we must give the ICO about a breach (see pg. 2&3)

 We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

 We know we must inform affected individuals without undue delay.

 We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

 We document all breaches, even if they don't all need to be reported.

Checklist

Reporting a breach

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA.

'Serious breaches' are not defined. However, the following should assist data controllers in considering whether breaches should be reported:

The potential detriment to data subjects:
The potential detriment to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriment includes emotional distress as well as both physical and financial damage.
Ways in which detriment can occur include:

- exposure to identity theft through the release of non- public identifiers, e.g. passport number;
- information about the private aspects of a person's life becoming known to others, e.g. financial circumstances.

The extent of detriment likely to occur is dependent on both the volume of personal data involved and the sensitivity of the data. Where there is significant actual or potential detriment as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report. Where there is little risk that individuals would suffer significant detriment, for example because a stolen laptop is properly encrypted or the information that is the subject of the breach is publicly-available information, there is no need to report.

The volume of personal data lost / released / corrupted:
There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise about what constitutes a large volume of personal data. Every case must be considered on its own merits.

Checklist

Example	☑ Reportable	✉ Not reportable
	Theft or loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of 100 individuals	Theft or loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the product being marketed

However, it will be appropriate to report much lower volumes in some circumstances where the risk is particularly high, perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether or not to report, the presumption should be to report.

The sensitivity of the data lost / released / corrupted: There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where that data is *sensitive personal data* as defined in section 2 of the DPA. Even a single record could be the trigger if the information is particularly sensitive.

Example	☑ Reportable	✉ Not reportable
	A manual paper-based filing system (or *unencrypted* digital media) holding the personal data relating to 50 named individuals and their financial records	A similar system holding the trade union subscription records of the same number of individuals, where there are no special circumstances surrounding the loss

Checklist

Method of reporting

Serious breaches should be reported to the ICO using our DPA security breach helpline on **0303 123 1113** (open Monday to Friday, 9am to 5pm). Select option **3** to speak to staff who will record the breach and give you advice about what to do next.

If you would like to report in writing you can use our DPA security breach notification form, which should be sent to the email address casework@ico.org.uk or by post to our office address *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.*

The security breach notification form can be found here: https://ico.org.uk/media/for-organisations/documents/personal-data-breach-report-form-web-dpa-2018.doc